PCT/GB2004/003541

GB0418541

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

PRIORITY DOCUMENT

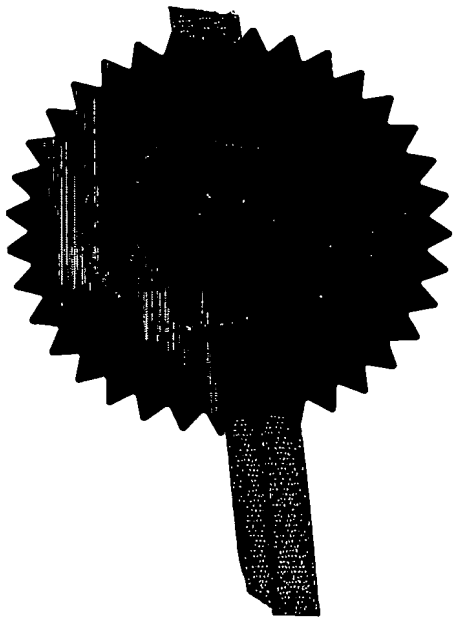
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

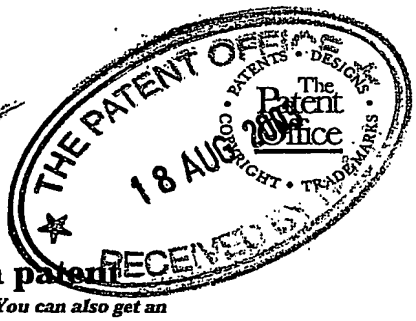


Signed Stephen Hordley

Dated 24 August 2004

Patents Form 1/77

Patents Act 1977
(Rule 16)



1/77

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales

19AUG03 E831181-2 D00850 800
P01/7700 0.00-0319363.8

1. Your reference

P85639GB00

2. Patent application number
(The Patent Office will fill in this part)

0319363.8

18 AUG 2003

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

CLEARSWIFT LIMITED
1310 Waterside
Arlington Business Park
Theale, Reading
Berkshire RG7 4SA

Patents ADP number *(if you know it)*

If the applicant is a corporate body, give the country/state of its incorporation

UK

8625527001

4. Title of the invention

EMAIL POLICY MANAGER

5. Name of your agent *(if you have one)*

Haseltine Lake

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Imperial House
15-19 Kingsway
London
WC2B 6UD

Patents ADP number *(if you know it)*

34001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*

a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

Yes

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	0
Description	10
Claim *(s)*	2
Abstract	0
Drawing *(s)*	2 x 2

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	1
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature: Hasselwelder — Date: 15 August 2003

12. Name and daytime telephone number of person to contact in the United Kingdom: Mrs J. McCormick — [0117] 910 3200

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 08459 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

EMAIL POLICY MANAGER

This invention relates to an email policy manager, for use in an email system. More particularly, the invention may be applied to a boundary agent, and a method used therein, for applying email policy.

Email is a convenient way for computer users to communicate, and in particular provides a very convenient way for a computer user to transmit data to another computer user.

However, this very convenience means that it is important for an organization to be able to carry out at least some forms of monitoring of emails sent from the organization. For example, emails may be used to send confidential information to unauthorized recipients outside the organization. As another example, emails may be used to send attachments in the form of program executables. This can lead to another difficulty arising from the use of email, namely the spread of computer viruses, which may be sent as executable file attachments to emails.

Many of these problems are solved to a large extent by the use of email manager software, that is, a software application which is provided on a local area network (LAN), and monitors emails. In particular, a boundary agent is a software application, which is provided on a local area network (LAN) having an internet connection, and monitors emails being sent over the internet by users connected to the LAN.

The boundary agent can then detect emails whose attachments may contain viruses. Similarly, the boundary agent can detect emails whose content is

suspicious. For example, emails containing specific key words can be regarded as suspicious. Also, emails having large attachments, or specific filetypes as attachments, can be regarded as suspicious.

Suspicious emails can be blocked, or they can be quarantined, that is, they are not transmitted at least until they have been reviewed. The rules, which are set up by the organization to determine which emails are treated as suspicious, are termed an "email policy".

Examples of boundary agents are products in the MIMESweeper® range from Clearswift Corporation.

One feature of boundary agents is that they can allow the email policy to be user-dependent. In particular, considering the application of the boundary agent to monitoring outgoing emails, the rules, which determine which emails are treated as suspicious, can vary from one user to another.

For example, while some personnel within an organization may be expected to send emails dealing with a particular subject, other personnel may not be expected to send emails dealing with that subject. In that case, emails containing key words relating to that subject may be treated as suspicious if they are sent by personnel within the second group.

Similarly, while some personnel within an organization may be expected to send emails with attachments of specific types, such as spreadsheets or image files, other personnel may not be expected to send emails having such attachments. In that case, emails having

that type of attachment may be treated as suspicious if they are sent by personnel within the second group.

Boundary agents applying such user-dependent email policies use the "From" field in the email message to identify the sender of the message, and then determine the rules which are to be followed for that user's messages.

However, this has the disadvantage that the content of the "From" field is no guarantee of the identity of the sender of the message. For example, a desktop email creating program may allow a user to create multiple accounts, and to complete the "From" field at will when creating such accounts. In this way, it becomes possible that, if a user knows the content of the "From" field in messages sent by another user, he can enter the same content in the "From" field of his own outgoing messages. The user is then subject not to the intended email policy, but to the email policy which applies to the other user.

It is known in other circumstances that digital signatures can be used to identify the sender of email messages. For example, US-5,956,408 describes a method for distributing data, in which data is encrypted using a private key of the data sender, and digitally signed by the sender. The recipient decrypts the encrypted data, using a public key of the data sender, and verifies the digital signature. If the digital signature is verified, the decrypted data is enabled for use.

However, as in the example given above, digital signatures are typically used only by a recipient of a message to confirm the identity of the sender or the

validity of the message, after the message has been transmitted across a network.

By contrast, according to an aspect of the present invention, there is provided a method of applying an email policy to determine whether a message should be allowed to be further transmitted across a network. The method according to the present invention applies a sender-dependent policy, using a digital signature to identify the sender of a message.

This has the advantage that the digital signature allows the sender to be identified with a high degree of certainty, so that the sender-dependent policy can be applied correctly.

According to another aspect of the present invention, there is provided a computer program product containing code for performing the method.

For a better understanding of the present invention, and to show how it may be put into effect, reference will now be made, by way of example, to the accompanying drawings.

Figure 1 is a block schematic diagram of a computer network.

Figure 2 is a flow chart, illustrating a method according to the present invention.

Figure 1 shows a computer network 10, which includes a local area network (LAN) 15, having personal computers (PCs) 16, 17, 18, 19 connected to it. The LAN has a connection to a wide area network (WAN) 25, which in this illustrated embodiment is the internet. Also

shown connected to the internet 25 is a further personal computer (PC) 30. It will be appreciated that a real computer network is very much more complex than that illustrated, but the network shown in Figure 1 is sufficient to illustrate and explain the present invention.

One common use of a computer network, such as that shown in Figure 1, is to transmit electronic mail messages. For example, the user of one of the personal computers 16-19 can transmit electronic mail messages to the user of the personal computer 30. Such messages can contain text alone, or they can have attachments in the form of computer files.

As shown in the Figure 1, the local area network 15 includes a boundary agent 32, which takes the form of software running on a mail server (not shown) in the network 15. The boundary agent 32 inspects the email traffic, which is intended to be transmitted over the internet 15. For example, the boundary agent 32 automatically checks mail messages for viruses.

In addition, the boundary agent 32 applies a sender-dependent email policy. Thus, while some personnel within an organization, that is, some users of personal computers 16-19, are permitted to send emails with attachments of specific types, such as spreadsheets or image files, other personnel are not permitted to send emails having such attachments. The boundary agent 32 can be generally conventional, and will therefore not be described further herein, except as required for an understanding of the present invention.

Figure 2 is a flow chart, showing a method performed by the boundary agent in accordance with the present invention.

In step 70, the boundary agent 32 inspects a mail message, which has been transmitted from one of the personal computers 16-19, intended for an external computer user, for example a user of the computer 30.

In step 72, the boundary agent 32 determines whether the message contains a digital signature and, if so, the boundary agent 32 determines in step 74 whether the digital signature can be verified.

A digital signature is a code which can be incorporated in an electronic mail message in order to identify the sender of the message. Conventional desktop email creating programs incorporate a feature allowing a digital signature to be added. As is known in the art, an infrastructure must be provided to allow the verification of digital signatures, and this will not be described in detail herein. Briefly, it is possible to verify a digital signature by checking with a Certification Authority, which maintains (either directly or indirectly) a list of valid digital signatures and the identities of the associated users.

If it is determined in step 72 that the message contains a digital signature, and if the digital signature is verified in step 74, the process passes to step 76. It should be noted that the verification of the digital signature may also confirm that the message has not been compromised during transport.

In step 76, the process applies a sender-specific email policy. That is, having extracted the purported

identity of the user from the message, and having verified that the digital signature applies to the same user, the boundary agent 32 determines whether the message, and any attachments, comply with an email policy which is specific to the user identified in the message. For this purpose, the boundary agent 32 maintains a list of users, and the respective email policies which are to be applied to messages sent by those users.

For example, while some users of the personal computers 16-19 may be expected to send emails dealing with a particular subject, other users may not be expected to send emails dealing with that subject. In that case, emails containing key words relating to that subject do not comply with the sender-specific email policy, if they are sent by personnel within the second group.

Similarly, while some users of the personal computers 16-19 may be expected to send emails with attachments of specific types, such as spreadsheets or image files, other users may not be expected to send emails having such attachments. In that case, emails having that type of attachment do not comply with the sender-specific email policy, if they are sent by users within the second group.

If it is determined in step 76 that the message complies with the sender-specific email policy, the process passes to step 78, and the message is allowed to be transmitted over the internet 25. By contrast, if it is determined in step 76 that the message does not comply with the sender-specific email policy, the process passes to step 80, and appropriate measures are applied.

For example, the message may be blocked, with or without notification to the sender, or may be quarantined for review by IT personnel responsible for operation of the local area network 15, or, in the case where it is an attachment which causes non-compliance with the email policy, the message may be transmitted without the attachment.

If it is determined in step 72 that the message does not contain a digital signature, or if is determined in step 74 that the digital signature is not verified, the process passes to step 82.

In step 82, the process applies a default email policy. The default email policy tests for specific keywords in messages, and for specific filetypes as attachments, in the same way as the sender-specific email policies described above. However, it is typically more restrictive in all respects than the sender-specific email policies applied to messages with verified digital signatures. That is, the default email policy may have a longer list of keywords which mark a message as non-compliant, or may regard more different filetypes as non-compliant.

If it is determined in step 82 that the message complies with the default email policy, the process passes to step 78, and the message is allowed to be transmitted over the internet 25, as described above. If it is determined in step 82 that the message does not comply with the default email policy, the process passes to step 80, and appropriate measures are applied, again as described above.

As mentioned above, the default email policy is typically more restrictive in all respects than the

sender-specific email policies applied to messages with verified digital signatures. Indeed, the default email policy may be such that no messages can comply with it. That is, all messages are rejected, unless they contain a verified digital signature.

It is also possible to define a variable default email policy. For example, a message without a digital signature may result from a simple omission. On the other hand, a message with a digital signature which does not match the purported sender identified in the message itself may be the result of a deliberate attempt to circumvent security procedures. Messages in these two categories may therefore be treated differently.

It is also possible to define a user-specific default email policy. For example, in the event that a message from one user or one of a group of users fails to include a verified digital signature, that message could be handled differently from a situation in which a message from another user or one of another group of users fails to include a verified digital signature.

The invention has been specifically described above with reference to its application in a boundary agent, to determine whether an email message can be transmitted across a boundary, for example to determine whether an email message can be transmitted outside a corporate local area network. However, it will be appreciated that the same method can be applied at any point in a network, for example within a local area network, to determine whether an email message can be further transmitted.

There is therefore disclosed a method of applying a sender-specific email policy based on a digital signature attached to an email message, to determine whether it should be transmitted further over a network.

CLAIMS

1. A method of applying a sender-specific mail policy, the method comprising:

maintaining a list of computer system users and associated sender-specific mail policies;

receiving a mail message intended for further transmission, the mail message indicating a sender thereof;

attempting to verify a digital signature in said mail message;

if the mail message does contain a verified digital signature, and if a user corresponding to the verified digital signature corresponds to the sender indicated in the mail message, applying an associated sender-specific mail policy to said mail message; and

if the outgoing mail message does not contain a verified digital signature corresponding to the sender indicated in the mail message, applying a default mail policy to said mail message.

2. A method as claimed in claim 1, wherein the step of applying a sender-specific mail policy to said mail message comprises determining whether the mail message complies with said policy;

if the mail message does comply with said policy, allowing transmission of said message; and

if the mail message does not comply with said policy, applying appropriate measures to said message.

3. A method as claimed in claim 1 or 2, wherein the step of applying a default mail policy to said mail message comprises determining whether the mail message complies with said policy;

if the mail message does comply with said policy, allowing transmission of said message; and

if the mail message does not comply with said policy, applying appropriate measures to said message.

4. A method as claimed in claim 1, 2 or 3, wherein said default mail policy is more restrictive than said sender-specific mail policy.

5. A method as claimed in claim 1 or 2, wherein the step of applying a default mail policy to said mail message comprises rejecting said mail message.

6. A method as claimed in any preceding claim, comprising receiving the mail message in a boundary agent, the mail message being intended for further transmission over an external computer network.

7. A computer program product, comprising code for performing the method as claimed in claims 1 to 6.

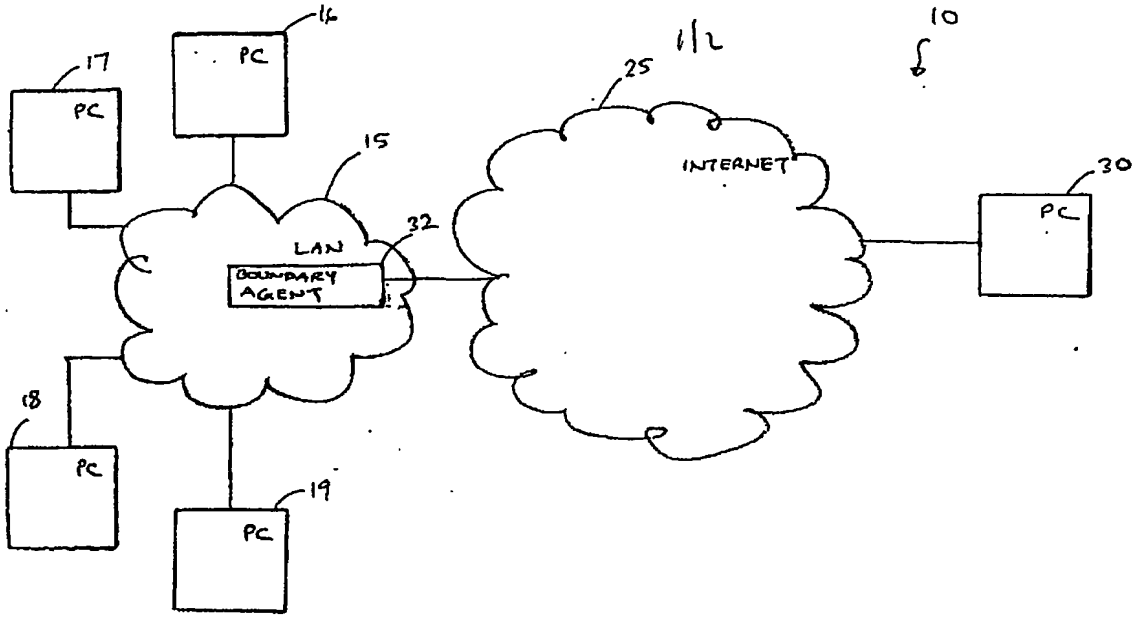

10
16
PC
17
PC
15
LAN
BOUNDARY AGENT
32
25
INTERNET
30
PC
18
PC
19
PC

FIG-1

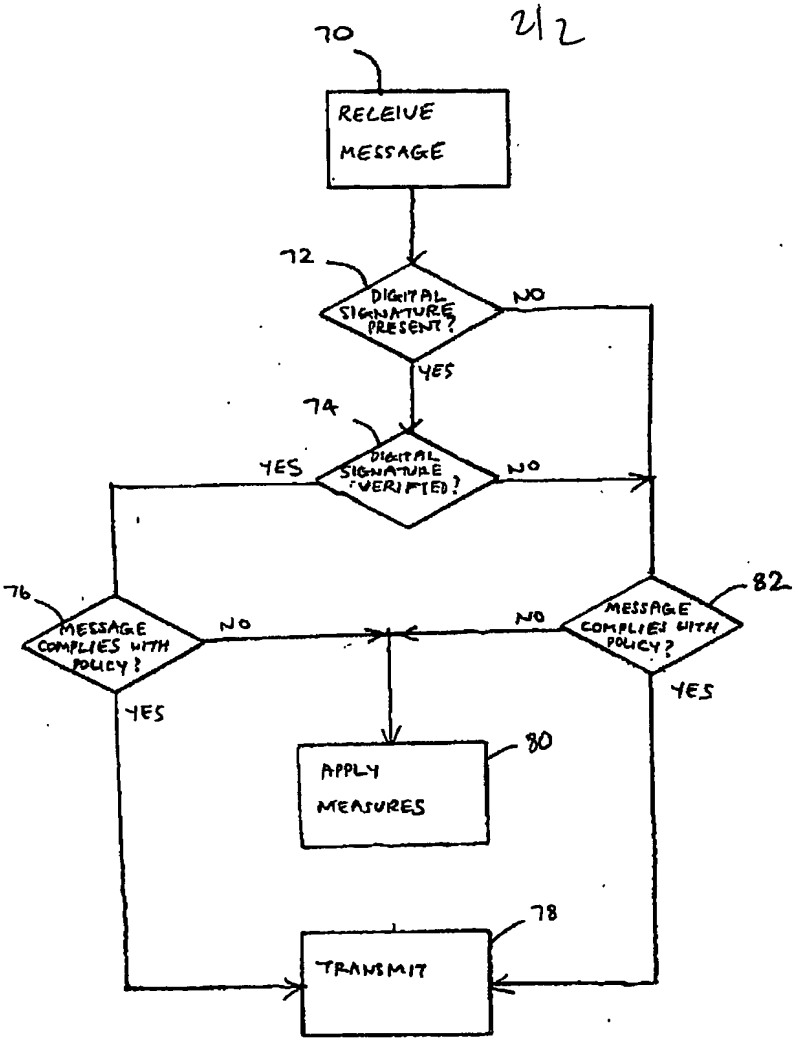

70
RECEIVE MESSAGE
72
DIGITAL SIGNATURE PRESENT?
NO
YES
74
DIGITAL SIGNATURE VERIFIED?
YES
NO
76
MESSAGE COMPLIES WITH POLICY?
NO
YES
82
MESSAGE COMPLIES WITH POLICY?
NO
YES
80
APPLY MEASURES
78
TRANSMIT

FIG. 2